EMPLOYEE PRIVACY NOTICE

How we use your personal information

Tomlinscote School is part of a multi-academy trust, The Prospect Trust. This privacy notice explains how we collect and process personal data relating to our employees to manage the employment relationship. The Trust is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations

Why we collect personal information

The Trust needs to process data to enter into an employment contract with you and to meet our obligations under your employment contract. For example, we need to process your data to provide you with an employment contract, to pay you in accordance with your employment contract and to administer benefit, pension and insurance entitlements.

In some cases, the Trust needs to process data to ensure that we are complying with our legal obligations. For example, we are required to check an employee's entitlement to work in the UK, to deduct tax, to comply with health and safety laws and to enable employees to take periods of leave to which they are entitled.

It is also necessary to carry out criminal records checks to ensure that individuals are permitted to undertake the role in question.

In other cases, the Trust has a legitimate interest in processing personal data before, during and after the end of the employment relationship. Processing employee data allows the Trust to:

- run recruitment and selection processes;
- maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights;
- operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace;
- operate and keep a record of employee performance and related processes, to plan for career development, and for succession planning and workforce management purposes;
- operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled;
- obtain occupational health advice, to ensure that it complies with duties in relation to individuals with disabilities, meet our obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled;
- operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that The Trust complies with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled;
- ensure effective general HR and business administration;

- provide references on request for current or former employees;
- respond to and defend any legal claims; and
- maintain and promote equality in the workplace.

Where the Trust relies on legitimate interests as a reason for processing data, we have considered whether or not those interests are overridden by the rights and freedoms of employees or workers and have concluded that they are not.

Some special categories of personal data, such as information about health or medical conditions, are processed to carry out employment law obligations (such as those in relation to employees with disabilities and for health and safety purposes). Information about trade union membership is processed to allow The Trust to operate check-off for union subscriptions.

Where the Trust processes other special categories of personal data, such as information about ethnic origin, sexual orientation, health or religion or belief, this is done for the purposes of equal opportunities monitoring.

What information does the Trust collect?

The types of information that we collect and process are listed below:

- your name, address and contact details, including email address and telephone number, date of birth and gender;
- the terms and conditions of your employment;
- details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with the Trust;
- information about your remuneration, including entitlement to benefits such as pensions or insurance cover;
- details of your bank account and national insurance number;
- information about your marital status, next of kin and emergency contacts;
- information about your nationality and entitlement to work in the UK;
- information about your criminal record;
- details of your working pattern (days of work and working hours) and attendance at work;
- details of periods of leave taken by you, including holiday, sickness absence, family leave and sabbaticals, and the reasons for the leave;
- details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence;
- assessments of your performance, including appraisals, performance reviews and ratings, training you have participated in, performance improvement plans and related correspondence;
- information about medical or health conditions, including whether or not you have a disability for which the organisation needs to make reasonable adjustments;
- equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief for statutory reporting purposes and;
- health & safety information in the form of risk assessments and accident at work reporting.

The Trust collects this information in a variety of ways. For example, data is collected through application forms or CVs; obtained from your passport or other identity documents such as your driving licence; from forms completed by you at the start of, or during employment (such as benefit nomination forms); from correspondence with you; or through interviews, meetings or other assessments.

In some cases, the Trust collects personal data about you from third parties, such as references supplied by former employers, information from employment background check providers and information from criminal records checks permitted by law.

Data is stored in a range of different places, including in your personnel file, in the Trust's HR management systems and in other IT systems (including the organisation's email system).

Who has access to data?

Your information will be shared internally, including with members of the HR team, Finance team, your line manager, managers in the business area in which you work and IT staff if access to the data is necessary for performance of their roles.

The Trust shares your data with third parties as follows:

- Companies you ask us to share your data with e.g. for references
- Upay cashless catering service
- ALPS for teaching staff data reporting purposes
- Cintra IQ to maintain and report employee information within our HR and payroll database
- Team Prevent (when you have been referred to occupational health)
- Local authorities (for statutory reporting purposes)
- Auditors
- Disclosure and Barring Service (DBS)
- Strictly Education 4s who act as an umbrella body in processing online DBS applications for the Trust.
- The National College (and similar organisations where it is identified as necessary for the performance of your duties)
- National Health Service (NHS)
- Any other organisation if access to your data is necessary for the performance of your duties

Further details of the third party privacy notices are available online or can be requested from the HR department.

Disclosure and Barring Service

The DBS has a number of service specific privacy policies. The policy for standard/enhanced disclosure checks explains how the DBS will use your personal data and outlines your rights under the GDPR. The DBS policy can be found here: https://www.gov.uk/government/publications/dbs-privacy-policies.

Applicants must make themselves aware of the policy and record that they have read and understood it before submitting a DBS application via the declaration sent out on application.

Babcock International Support Services Ltd acts as an umbrella body in processing online DBS applications on behalf of the Trust,

The Trust also shares your data with third parties that process data on its behalf, in connection with payroll, the provision of benefits and the provision of occupational health services.

Google

Your data may be transferred to countries outside the European Economic Area to Google:

The Prospect Trust uses Google mail applications which may store data outside the EEA.

Google is an international organisation and in order to provide you with access to Google services your data may end up being transferred to a data center outside of the EEA. Google's privacy policy can be found here: https://privacy.google.com/intl/en-GB/index.html

Other service providers used by the Trust may also transfer or store data outside of the EEA. In such cases, it will only be where the destination country has been declared by the European Commission as having adequate levels of protection or where adequate and appropriate safeguards are in place.

How does the Trust protect data?

The Trust takes the security of your data seriously. The Trust has internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by its employees in the performance of their duties. Data sharing agreements are in place with organisations that we share your personal data with and the transfer of data is sent securely.

Where the Trust engages third parties to process personal data on its behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

How long we keep your personal information

We will keep your information for as long as you are an employee of The Prospect Trust and then for the following timescales and reasons after your employment has ceased:

- Employee records will be held for 6 years after employment has ended for the purpose of providing references; to meet legislative requirements, for data analysis and statistical reporting purposes.
- Disciplinary and grievance data will be destroyed after the time limit stated has been spent
- Maternity/paternity and any other family leave data will be destroyed three years after employment has ended
- Recruitment data for unsuccessful applicants to the College will be held for six months to meet legislative requirements and to respond to any questions or complaints
- Health & Safety accident at work reports will be held for three years in the event of a civil claim and 40 years for COSHH (Control of Substances Hazardous to Health) claims.
- DBS forms will be held on file for a period of six months, in line with the DBS code of practice and retention guidelines.

Staff records will be destroyed once the retention period has expired. The latest version of any approved retention schedule will always be published online within Trust Academies.

How we use your information for automated decision-making

Recruitment processes are not based solely on automated decision-making.

How we use your information for profiling

We do not use data for profiling purposes.

Your rights

As a data subject, you have a number of rights. You can:

- access and obtain a copy of your data on request;
- require the Trust to change incorrect or incomplete data;
- require the Trust to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing;
- object to the processing of your data where the Trust is relying on its legitimate interests as the legal ground for processing; and
- ask the Trust to stop processing data for a period if data is inaccurate or there is a dispute about whether or not your interests override the organisation's legitimate grounds for processing data.

If you would like to exercise any of these rights, or make a subject access request, please contact dpo@farnborough.ac.uk

If you believe that the Trust has not complied with your data protection rights, you can complain to the Information Commissioner.

What if you do not provide personal data?

You have some obligations under your employment contract to provide the Trust with data. In particular, you are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith. You may also have to provide the Trust with data in order to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to provide the data may mean that you are unable to exercise your statutory rights e.g. maternity leave and pay.

Certain information, such as contact details, your right to work in the UK and payment details, have to be provided to enable The Trust to enter a contract of employment with you. If you do not provide other information, this will hinder the Trust's ability to efficiently administer the rights and obligations arising as a result of the employment relationship efficiently.

How to complain

Please let the Trust know if you are unhappy with how we have used your personal information.

In the event that you wish to raise a complaint in relation to your data; complaints should be made to the Data Protection Officer: dpo@farnborough.ac.uk

If the Trust are unable to resolve your complaint, you have the right to lodge a complaint with the Information Commissioner's Office.